Custom Solutions for Diverse Needs: Laying the Foundation for Tailored SETA Programs in the Healthcare Domain

Florian Rampold
University of Goettingen
florian.rampold@uni-goettingen.de

Julia Heinsohn
University of Goettingen
julia.heinsohn@stud.uni-goettingen.de

Florian Schütz
University of Goettingen
florian.schuetz@uni-goettingen.de

Julia Klein
University of Goettingen
julia.klein@uni-goettingen.de

Thomas Keller
University of Hohenheim
thomas.keller@uni-hohenheim.de

Kristin Masuch
University of Goettingen
kristin.masuch@wiwi.uni-goettingen.de

Julia Warwas
University of Hohenheim
julia.warwas@uni-hohenheim.de

Abstract

In recent years, the number of data breaches in the healthcare sector has steadily increased. As a result, security, education, training, and awareness programs are recognized as an integral part of educating employees about security threats. Although these programs are considered commonplace in many organizations, they often follow one-size-fits-all approaches that could hinder the success of security training. In this study, we address this issue by conducting a domain analysis for IT-secure behavior in healthcare using the evidence centered assessment design. We define the representative target group as caregivers and physicians in hospitals. Subsequently, we observe the work tasks and assets of both job profiles in three hospitals in Germany to determine the most relevant security threats in the domain. In this way, we extend the cyber security domain model of Schuetz et al. (2023) and pave the way for developing tailored SETA programs in the healthcare domain.

Keywords: SETA, Evidence Centered Assessment Design, Domain Analysis, Observational Study, Risk Assessment

1. Introduction

The healthcare sector is a popular target for data breaches. This costs nearly $7 million per data breach – the highest average cost of any industry for the 12th consecutive year (IBM Security, 2019). Security education, training, and awareness (SETA) programs are one intervention that may reduce the risk of being breached as they strengthen employees' competencies in dealing with security threats (Hu et al., 2022; Thomson & Von Solms, 1998). While the overall purpose of SETA programs is considered essential to protecting organizations from data misuse, economic and financial loss, or information theft, the effectiveness of these programs is sometimes called into question (Hu et al., 2022; Tsohou et al., 2015). One reason for this may be the "one-size-fits-all" approach to educating employees on security-related topics (D'Arcy & Hovav, 2009; Dincelli & Chengalur-Smith, 2020), which can be problematic for two reasons.

First, these programs are often not tailored to employees' actual demands and needs (Willison & Warkentin, 2013), especially in the healthcare context. Thus, it is ignored that employees work in different contexts and that the situations that pose a security risk in day-to-day work can vary across companies and professional occupations. Second, employees might not fully understand the importance of information security because they cannot comprehend the purpose of the training content due to a lack of relevance to their day-to-day work (Hu et al., 2022; Rampold et al., 2022).

Therefore, vocational education and training (VET) research indicates that learning contexts should be aligned to situational action-taking to raise competent employees (Winther, 2010). Competence is often considered a multidimensional construct encompassing the cognitive abilities, skills, and motivational dispositions required to perform domain-related tasks in a wide variety of circumstances (Blömeke et al., 2015). Hence, competence captures the demands and

URI: https://hdl.handle.net/10125/106832
978-0-9981331-7-1

requirements that employees in different domains need to possess for successful action-taking (Rampold et al., 2022). However, detailed knowledge of the underlying domain is needed to holistically assess employees' information security competencies. One approach to tackle this challenge in VET is to conduct domain analyses that comprehensively overview the working tasks and contents that are prerequisites for modeling the required domain-specific competencies of employees (Seeber, 2016). For example, Seeber (2016) conducted a domain analysis to record the daily working requirements of medical assistants.

Schuetz et al., (2023) instead performed a domain analysis relating to IT-secure behavior. Their results indicate that security threat areas and events can classify security threats. The authors provide a thorough classification framework including 1,087 security threats to which employees can be exposed in the organizational working context.

However, the identified security threats are broad and need to be contextualized for building tailored SETA programs or assessing the information security competencies of employees in the healthcare context. Studies have shown that the healthcare sector differs from other domains. This is mainly for two reasons. First, the healthcare sector deals with susceptible and valuable data, such as patient medical records, personal information, and financial information (Martin et al., 2017). Second, studies indicate that critical infrastructure is the second most important driver in the industry after the Internet of Things (Statista, 2017). Thus, employees working in the healthcare domain require specialized and deep knowledge and expertise to secure health-specific assets effectively.

In this study, we are therefore interested in the security threats that pose a risk in the domain of IT-secure behavior in healthcare. Hence, our work is guided by the following research question:

Which job profiles and security threats should a domain model for IT-secure behavior consider in healthcare when developing tailored SETA programs?

We address this research question by following the guidelines for conducting a domain analysis based on the Evidence Centered Assessment Design (ECD) by Mislevy et al. (2006). The domain analysis is based on Schuetz et al. (2023) and consists of three phases. First, we defined the target group (physicians, caregivers) and the objects to be classified (security threats) in the domain based on scientific and practical literature. Second, we derived an exhaustive list of security threats relevant to the domain based on literature analysis. We then conducted 11 observational studies to get an in-depth view of the working tasks and critical assets of employees in German hospitals in the identified target groups. We assessed each working task with its involved assets and mapped security threat events to the assets. As a result, we inferred the security threats most relevant to training in SETA programs in the healthcare context. Finally, we assessed the risk of the most impactful security threats employees can face in their working context by conducting a group interview with eight chief information security officers (CISOs) of German hospitals. The result is a classification of the ten most relevant security threats for both defined job profiles that are relevant to be addressed as a sound basis for SETA programs in the healthcare domain.

Our contributions to this work are manifold. First, we follow calls for research to promote more tailored SETA programs beyond one-size-fits-all approaches. Second, we extend the cyber security domain model (CSDM) by Schuetz et al. (2023) to the healthcare domain. By doing so, we add 33 security threats to the domain model. Third, our research provides a feasible number of security threats relevant to be addressed in healthcare-specific SETA programs.

2. Research Background

2.1. SETA Programs and Security Threats in Extant Literature

In a recent study about the nature of SETA programs, Hu et al., (2022, p. 754) define SETA based on multiple studies as “ongoing efforts that promote employees’ consciousness of security issues and provide them with general security knowledge and skills to combat security threats and risks”.

In the last 30 years, previous research has mainly focused on SETA programs' effectiveness or design criteria that lead to improved intervention outcomes. Commonly, the effectiveness is evaluated based on the influence of the existence of SETA programs on changing security compliance intentions (D’Arcy & Hovav, 2009; Talib & Dhillon, 2015). A few studies extend this procedure by observing the intervention design for particular security threats (such as social engineering and phishing) to enhance the intervention effectiveness (Dincelli & Chengalur-Smith, 2020; Silic & Lowry, 2020). Security threats are adverse incidents compromising the integrity or confidentiality of organizational assets, individuals, or organizations (Blank & Gallagher, 2012; Gerić & Hutinski, 2007; Schuetz et al., 2023).

Several research studies suggest group-based learning based on participants’ starting points (Caldwell, 2016; Heikka, 2008). Moreover, few papers stress the importance of designing SETA programs for different target audiences (Heikka, 2008; Thomson & von Solms, 1998). Multiple researchers also emphasize the importance of fitting the content to individual

employee needs (Goode et al., 2018; McCrohan et al., 2010). Although many research papers have suggested recommendations for the conceptualization and design of SETA programs (Goode et al., 2018; Tsohou et al., 2015), limited research addresses the differential relevance of varying security threats for different target domains that can overcome the challenges associated with one-size-fits-all approaches.

2.2. Domain Analysis as Part of the Evidence-Centered Assessment Design

One central objective of VET research is developing and accessing vocational competence (Klotz et al., 2015). Competence is a complex construct composed of underlying cognitive and affective/motivational states that act as a disposition for observable behavior in varying contexts (Blömeke et al., 2015). ECD is a prominent method of designing educational assessments that can capture vocational competence in a particular domain (Seeber, 2016).

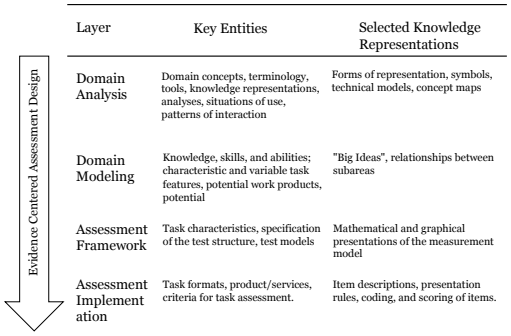

Figure 1 ECD Framework (reprinted from Schuetz et al., 2023, based on Mislevy & Haertel, 2006 and Seeber, 2016)

In these terms, a domain encompasses a specific context where individuals or entities interact and engage in activities relevant to that subject area (Klieme et al., 2003; Schuetz et al., 2023; Seeber, 2016). ECD understands assessments as evidentiary arguments that aim to measure an underlying target group's knowledge, skills, and abilities (Mislevy, 2013). It is divided into four layers that define the sequential process of setting up this assessment as realistic and authentic as possible (see Figure 1). The first step in the ECD framework is the domain analysis. Domain analysis forms the basis of subsequent evidence-based assessments. It aims to collect and connect information within a specified domain (Mislevy, 2013; Mislevy & Haertel, 2006). Information can be reflected via various constructs, such as content, theories, terminologies, concepts, and representational forms of a domain, which can typically be observed across domain-specific situations (Winther, 2010). Thus, domain analysis concerns the interaction of persons in the domain with their working environment and other persons. These insights are then enhanced by a deep understanding of the tasks, knowledge representations, and tools required to achieve satisfactory results in the given domain. (Mislevy 2013). Various methods can be used to gather this information about the domain, such as document analysis, analysis of job advertisements, review of professional practice curricula, ethnographic studies, observations, and expert interviews (Mislevy, 2013; Seeber, 2016). In the subsequent domain modeling phase, the results from the domain analysis are structured and prepared for evidence-based assessments. This step is necessary to build a conceptual framework that defines the competencies needed to assess the observed tasks and contents derived from domain analysis in an assessment framework (Mislevy, 2013; Mislevy & Haertel, 2006). Once the domain model has been created, a competence model can be specified from the theoretical assumptions about professional competencies (Seeber, 2016). An exemplary competence model from Seeber's study contains various dimensions reflecting three different areas of activity as subdimensions of the identified professional competencies (Seeber, 2016). The domain and competence models are translated into measurement models, scoring methods, and delivery requirements in layer three. Finally, in layer four – the assessment implementation – the operational elements from the conceptual assessment framework are constructed and initiated (Mislevy, 2013).

The ECD framework informs our research in the following way. It provides a blueprint for a thorough analysis of the domain. We argue that IT security in domains such as finance or health can vary due to the used assets and security threat events that pose a different risk depending on the domain. In VET research, it is common to distinguish between these domains when developing assessment tests of competence (Seeber, 2016).

3. Domain Analysis in Healthcare

In this study, we conducted a domain analysis for IT-secure behavior in the healthcare context. In these terms, our procedure in this work is threefold and based on the CSDM development process of Schuetz et al. (2023). First, we identified the objects and actors in the domain. Second, we analyzed the identified object in the domain of IT secure behavior in healthcare. Third, we reduced the objects by conducting observational studies to identify irrelevant objects. The classification of Schuetz et al. (2023) informs the list of assets we acquired for the observational studies. Figure 2 shows the process.

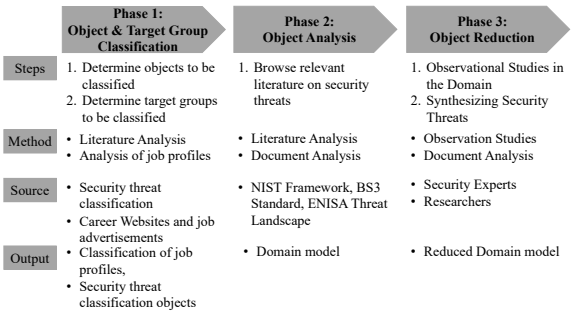

Figure 2 Research Approach (based on Schuetz et al., 2023)

3.1. Phase One: Classification of Objects and the Target Group in the Domain

The first step in developing the domain model is identifying and classifying the relevant objects and target groups of interest. First, security threats needed to be defined to enable a further investigation of relevant threats in the domain. Second, the objects that need to be identified in this step are the various job profiles that represent the actors in the domain of IT-secure behavior in the healthcare context. Several steps were taken to accomplish this, as described below.

Classification of Security Threats: In the first phase of our applied methodology, we followed the approach of Schuetz et al. (2023). The authors have conducted a thorough classification of security threats (also referred to as security threat vectors) that are composed of two dimensions: security threat areas and security threat events (see Schuetz et al. (2023) for detailed information). Each threat event can be classified into one of four subdimensions: adversarial (e.g., social engineering attack), accidental (e.g., spilling of sensitive information), structural (e.g., outdated hardware), or environmental (e.g., earthquake, fire) (Blank & Gallagher, 2012). While related security threat classifications, such as Jouni et al. (2014), consider the threat source as a standalone dimension, we agree with Schuetz et al. (2023) that the threat source is not relevant when building a domain model for IT-secure behavior in the healthcare context. It is reasonable for companies to distinguish between different threat sources. However, the employee needs to recognize the threat event (for example, a phishing email) without needing to know the type of attacker (Schuetz et al., 2023).

The threat area dimension, developed by Gerić and Hutinski (2007), helps to understand the domains in which security threats might be present. It allows organizations to conduct effective risk assessments and identify generic threat events. To ensure that these events can be effectively addressed, organizations must also consider how these threats can affect the assets they possess (Blank & Gallagher, 2012). Like Schuetz et al. (2023), we consider the assets part of a security threat. Assets can be either physical (e.g., persons, organizations, computing devices, information technology, hardware) or non-physical (software, data) entities that are of value to an organization (Wunder et al., 2011).

Classification of the Target Group: After we defined the objects of interest to be investigated in the domain analysis, we needed to define a target group that was representative of different job profiles in the healthcare context. Scientific literature and practice-related sources were examined to categorize job profiles in hospitals. The literature search revealed that a distinction is predominantly made between the superordinate job profiles of administrative staff, physicians, and caregivers (Bräutigam et al., 2014; Chiou et al., 2014; Drevin et al., 2017; Kvist et al., 2013; Maseti & Pottas, 2006). For validation, this categorization was compared with healthcare occupations presented by hospitals on their career websites. In total, 50 job advertisements were analyzed to ensure that the categorization based on the two job profiles was relevant to the research objective. Thus, the following professions were taken into account: Medical Assistant (MA), Medical-Technical Assistant (MTA), Assistant Physician, Senior Physician, Caregiver, Office Assistant, Human Resources Assistant, and Public Relations Assistant.

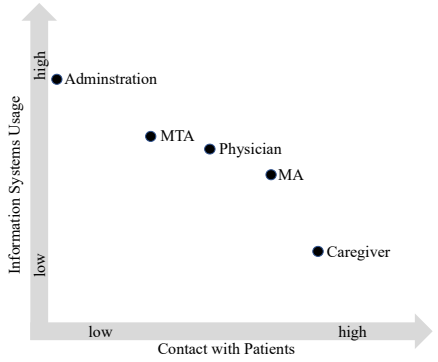

Figure 3 Classification of Job Profiles

By combining the results from scientific publications and practice-related sources, five superordinate job profile bundles can be identified: physicians, caregivers, administrative staff, MTA, and MA (depicted in Figure 3). In addition to the specific fields of activity, the five job profile bundles described above differ in two further dimensions: contact with patients and the intensity of using information systems. The categorization serves to improve the analyzability of the possible threat potential in the individual job profiles in healthcare. This classification was evaluated

through job profile descriptions on career websites and several interviews with two persons in the role of CISOs in German hospitals.

The results suggest that the job profiles of MTA, physicians, and MA are very similar regarding patient contact and the intensity of using information systems. However, as administrative staff is not a healthcare-specific occupation and our research goal is to extend the CSDM of Schuetz et al, (2023) to the healthcare domain, we excluded administration from further investigation. Physicians and caregivers differed the most in their different characteristics in dealing with information systems and patient contact. Thus, the two job profiles were assumed to be representative of the healthcare domain in the course of the analysis.

3.2. Phase Two: Literature-based Identification of Objects in the Domain Analysis

First, we created a list of threat areas and events that build security threats, as discussed in phase one. To do this, we used the security threat classification of threat areas and threat events from Schuetz et al. (2023) as a basis. We then extended both lists by investigating healthcare-specific security threat events and security threat areas using documents and literature. Schuetz et al. (2023) include 85 threat events based on the NIST publication 800-30 in the literature search (see Blank & Gallagher, 2012). As this publication's list of threat events is extensive but not specific to the healthcare context, we aimed to find more unique threat events for the healthcare domain. Therefore, we included threat events from the B3S industry standard and the ENISA publication for smart hospitals (ENISA, 2016). The final set covers 103 threat events. Based on multiple resources (e.g., Biener et al., 2015; Lehner, 2021), Schuetz et al. (2023) specify 43 relevant assets to consider in the domain of IT-secure behavior. Similarly, we extended the list by consulting the B3S industry standard. The final list includes 50 distinct threat areas.

3.3. Phase Three: Reduction of the Objects in the Domain

Although the predefined domain model is exhaustive, a combination of threat events and areas leads to 5,150 security threats potentially being relevant to IT-secure behavior in healthcare. This extends the CSDM of Schuetz et al. (2023), who identified 3,655 security threats. Since we aim to identify security threats that can provide input for tailored SETA programs in the healthcare context, we decided to prioritize the results from the literature-based analysis by obtaining qualitative data through observational studies in hospitals as representative of the healthcare domain.

Observational Studies in Hospitals: After creating a list of possible relevant threat areas (assets) and threat events, the initial domain model was contextualized using observational studies to specify relevant security threats in the domain of IT-secure behavior in the healthcare context. The observational studies had two primary goals. As it is impossible to directly observe security threats in the daily working routine of hospital employees, the observations were concerned with identifying the respective work tasks in the various job profiles. Second, within the work tasks, the aim was to identify the assets (threat areas) that could potentially become the target of a security threat event (see Schuetz et al., (2023)) through attackers or inadvertent misconduct. This procedure allowed us to eventually define the security threats most relevant to address in SETA programs within the domain.

Observation is a data collection method within qualitative research (Bowling, 2014). Qualitative research methods are advantageous when there is little prior knowledge and sensitive or complex issues (Bowling, 2014). They can also enhance quantitative research by placing quantitative data in a logical social context through qualitative surveys (Bowling, 2014). In observational studies, researchers perceive ongoing processes in a natural setting (Göran, 2019). The observing person takes field notes (jottings) to capture what happens in the setting (Göran, 2019).

Commonly, a distinction is made between direct and participant observations (Göran, 2019). In the study conducted, the observer has taken the role of observer-as-participant. This type of observation not only allows one to observe the activities that occur during the observation but also to conduct short interviews with the observed persons (Baker, 2006). In addition to the assignment of the observer as observer-as-participant, the study was conducted as a hidden observation. Although the observation could not occur from a hidden place, the observed persons were nevertheless not informed in more detail about the purpose of the observation. A mixture of structured and unstructured observation was used to document the observations so that structured data on the use of equipment could be collected. However, the observers also had the freedom to collect additional information. In this way, the type of survey follows the suggestions for a semi-structured observation (Denscombe, 2017; Sarantakos, 1998). Before the observational studies were conducted an ethical review board of the university in lead approved the procedure.

During this work, persons with caregiver and physician job profiles were observed in their natural work settings. Each observation lasted four hours. The

observations were conducted in three hospitals in Germany (see Figure 4 below).

Job Profile	Job Position	Gender	Age
Physician	Senior physician	Female	48-57
	Chief physician	Male	28-37
	Assistant physician	Female	28-37
	Senior chief physician	Female	28-37
	Physician specialist	Male	38-47
	Physician specialist	Male	28-37
	Physician specialist	Male	28-37
Caregiver	Caregiver staff	Male	28-37
	Caregiver staff	Female	18-27
	Caregiver staff	Male	28-37
	Caregiver manager	Female	28-37

Figure 4 Observational Studies Participants

We used the identified security threat areas and events identified in phase two as input for the observational studies. Each observer received both lists as a guide to what to look for in the observations. Seven observations were conducted for the physician job profile. In addition, four observations were conducted for the caregiver job profile. From the observations, eleven work tasks could be defined, including six tasks for the physician job profile and five for the caregiver job profile. For the caregiver job profile, the following work tasks were identified: work with patients, documentation of work with patients, organizational tasks, nursing area management, and non-work-related tasks. Figure 5 presents two observed work tasks with four exemplary jottings (J1- J4) and the associated assets for the job profile caregiver.

	Work Task	Jottings	Involved Assets (Threat Area)
J1	Organizational tasks	The caregiver's organizational duties include handling various calls from internal positions in the hospital to (e.g., physicians, floor office).	Employee Mobile phone
J2		After working on the computer, the screen is not locked in most cases. The automatic lock takes longer than 5 minutes.	PC Laptop
J3	Documentation of work with patients	After patients have been cared for by the caregiver, he or she enters all information about it into the PDMS and the HIS. The systems are used frequently.	PDMS HIS
J4		There is a notice at the bottom left of the mobile PC screen (pw: ...-1211...!). There are also two USB ports on the mobile PC.	USB Flashdrive PC Laptop

Figure 5 Exemplary Results for Caregivers

In detail, the following work tasks were defined for physicians: work with patients, documentation of work with patients, organizational tasks, communication (internal and external), scientific work, and non-related work tasks. Non-work-related tasks mainly referred to tasks that were not part of the employees' activities and duties but were still observed. One example is the use of smartphones and other devices for personal purposes. Next to the work tasks, we captured special situations from the *work environment* for both job profiles. For each identified work task, jotting notes were conducted to record the behavior of the observed persons that can lead to a potential security threat. Additionally, the involved assets during the work tasks were noted.

Synthesizing Potential Security Threats from the Observations: Once the work tasks for the two job profiles have been defined, relevant threat vectors were inferred from the observed assets and the work tasks. For this mapping, environmental threat events were excluded in advance for assessment. According to ENISA (2016) and Motevali Haghighi and Torabi (2020), these threats are less likely to occur than others. The mapping was done by three researchers using a majority vote and refers only to the observable situations and the information that could be obtained through inquiries. When there was a disagreement between the researchers, we kept the threat vector in the model since we were interested in as many reasonable combinations of threat events and areas that build a threat vector. Our reduced domain model for IT secure behavior in the healthcare domain holds 114 security threats as described below.

A total of 54 threat vectors were assigned to the caregiver job profile. Most of these vectors relate to the *documentation of work with patients*. The 20 identified security threats primarily relate to working with the patient data management system (PDMS) and hospital information system (HIS). Since caregivers must also electronically enter all patient-related activities into these systems, many security threats arise, such as denial of service attacks, insertion of malware and malicious software, insertion of false but credible data, and mishandling and contamination of sensitive data. Since the mobile PCs used for work were observed to have USB ports, this also makes them a potential gateway for attackers. The same applies to employees' notes on their screens with passwords. This, in turn, enables brute force attacks.

The *organizational tasks* that caregivers are required to perform also elicit threats. Seven threat vectors have been identified. Although emails are rarely sent, general communication via email creates some of the threats identified. Examples include (spear) phishing, malware, and network traffic modification. In addition to the threats from documenting work with patients, four threat vectors were identified for the caregiver job profile for the *work with patients*. Caregivers were observed to use their smartphones often and wear a smartwatch during work hours, leading to 14 security threats in *non-work-related tasks.* Captured

situations include posting photos from the nursing area and sending data about patients via messenger services. Examples of threat events include the dissemination of sensitive information, the use of publicly available information for subsequent attacks, and the interception of data through inadequately encrypted communications.

For the physician's job profile, 60 security threats emerged from the mapping procedure. Most of the threat vectors were also assigned to the work task *documentation of work with patients*. The 20 threat vectors identified are mainly related to working with the HIS and SAP. Since physicians have access to these information systems, where they enter data concerning the patient or query data from the digital patient record, many threats arise, resulting from both intentional and unintentional behavior. Another threat vector in this environment is the internet browser, as physicians frequently use this for research. Associated threats include the insertion of malware and falling for fake websites. In addition to the operation of medical information systems, threats arise from using medical devices (e.g., point-of-care electronic devices) assigned to the *work environment*. An attacker can use these devices as a gateway for various attacks.

Moreover, threats arise from physicians talking to their patients in the office, giving the patient access to files and devices scattered around the room. Finally, the confidentiality of patient information must be maintained to prevent it from falling into hostile hands. Open communication about and with patients in the hallway poses a risk that should be addressed if necessary.

Physicians also perform *organizational tasks* that are mainly conducted using the stationary PC. In this case, they are prone to social engineering attacks, such as shoulder surfing through unlocked screens and brute force login attempts. Nine security threats also arise from communication with external and internal parties, posing significant security threats. There are nine threats associated with the *communication of work tasks*. These are mainly related to email communication. (Spear) phishing attacks, malware, network traffic modification, and social engineering attacks can be relevant threat events. An attacker can use communication via telephone, instant messenger (e.g., WhatsApp), and email to initiate one of these threat events. In addition to the previous threat vectors, nine threats were identified for *non-work-related tasks* related to using smartphones or computers for personal purposes. Examples of potential threat events include malware, compromising these devices, and intercepting unencrypted communication traffic. In addition, using messaging services to communicate with other physicians poses a risk of exposure to personal information. Moreover, eight threat vectors could be assigned to the *work environment*. The threats mainly relate to employees or physical parameters (e.g., doors) as threat areas and arise from inadequate access controls. For example, threats can emerge since data can be stolen. Lastly, four threat vectors were identified for the *scientific work* of physicians. Due to increased internet research, malware and falling for duplicate websites pose a significant threat. Furthermore, spear phishing is relevant because physicians receive many emails due to their general communication with students or researchers and may be susceptible to personalized spear phishing attacks. As a last step, we compared the 114 security threat vectors with the threat vectors identified in the CSDM of Schuetz et al. (2023). By conducting observational studies, we were able to extend the CSDM by 33 threat vectors that are especially relevant in the healthcare context. Thus, the extended CSDM contains 1,120 total threat vectors.

4. The CSDM for Healthcare Applied

Although the domain model covers many security threats applicable to healthcare, some security threats might be more relevant to be addressed in SETA programs than others. Hence, in the final step of this work, we showcase how the CSDM for healthcare can be applied to craft SETA programs tailored to the healthcare domain. To do so, we followed a two-way procedure. Since most threat events were taken from the list in NIST publication 800-30 (Blank & Gallagher, 2012), the qualitative scale taken from that publication was also used to analyze and evaluate the risks. In contrast to the NIST publication, this work does not consider the likelihood and impact of the threat event but rather the likelihood and severity of the threat vector (Schuetz et al., 2023). Each researcher independently assessed the risk of the 114 threat vectors identified in the observational studies and then mutually determined the risk assessment with a majority vote. This approach enabled the researchers to make accurate and informed decisions regarding the security risk posed by each threat vector. Table 1 shows the NIST assessment scales and their calculation logic. The overall likelihood is composed of the likelihood of occurrence/initiation of the threat vector and the likelihood of the threat vector resulting in adverse impacts. The result of the overall likelihood can then be taken from the NIST assessment scale tables (Blank & Gallagher, 2012). In the next step, the level of impact is determined. The combination of overall likelihood and level of impact then results in the overall risk for the security threat vector. The risk assessment approach resulted in 15 security threats with a high or very high risk for caregivers. Instead, 27

security threats were found to pose a high or very high risk in the working context of physicians.

Table 1 NIST Risk Assessment (based on Blank & Gallagher 2012)

NIST Assessment Scale	Threat Vector
1: Likelihood of Occurrence/Initiation	High
2: Likelihood of Adverse Impacts	Very High
3: Overall Likelihood (1*2)	Very High
4: Level of Impact	Moderate
5: Level of Risk (3*4)	High

As a last step, we evaluated the risk assessment outcome by conducting a group interview with eight CISOs from German hospitals. Before we ran the group interview, each CISO ranked the security threats for both job profiles based on their criticality. The CISOs were also allowed to create security threats not considered in the domain model. During the group interview, the list of security threats was reduced to ten security threats for each of the two job profiles. By doing so, we propose a parsimony and feasible classification of security threats that are beneficial to consider when developing SETA programs in healthcare or hospital-related domains. The resulting security threats composed of threat area (asset) and threat event can be found in the appendix (see Figures 6 and 7). Although we identified similar work tasks for physicians and caregivers, the most critical security threats for both job profiles differ. While caregivers mainly work with the PDMS, physicians more frequently use the HIS. Moreover, caregivers are more often in touch with patients. Thus, the risk of spilling sensitive information is higher. Instead, in most cases, physicians have more access rights to the internet. As a result, highly relevant security threats such as spoofing, and insertion of malware emerge.

5. Discussion

In this research, we conducted a domain analysis for IT-secure behavior in the healthcare domain. Our study provides several contributions to both information security and VET research. First, we follow the calls to shape the development process of more tailored SETA programs that go beyond one-size-fits-all approaches. Our domain model holds a feasible number of security threats that can be used for either information security competence assessments or as input to build targeted SETA programs. Second, we extend the CSDM by Schuetz et al. (2023) applied to the healthcare domain. By doing so, we add 33 threat vectors to the CSDM and follow the demand of Schuetz et al. (2023) to tailor the classification framework to specific domains. Third, applying the CSDM for healthcare indicates that security threats are embedded in different work tasks. This is particularly relevant to IT security competence assessments and subsequent SETA development processes targeted to specific peer groups such as physicians and caregivers. Fourth, our results of the 20 most critical security threats in healthcare can be used as input for future studies investigating SETA effectiveness in varying contexts.

In addition to the theoretical implications, the results may also be helpful to various stakeholders in practice. First, stakeholders in the healthcare domain, such as hospitals, can use the top ten identified security threat vectors to measure the security competencies of their employees regarding IT secure behavior. This in turn can reduce security risk exposure (Schütz et al., 2023). By differentiating the SETA programs according to occupational profiles, employees are more likely to follow the contents of the training courses with greater attention, resulting in higher acceptance of the courses (Schuetz et al., 2023). Moreover, the CSDM for healthcare can be leveraged to build tailored SETA programs that are closely aligned to the target groups' (physicians and caregivers) working tasks.

Our study holds a few limitations that are discussed in the following. First, we limited the target group of the domain to two job profiles. Based on our argumentation, physicians, and caregivers build a representative sample of distinctive groups within the healthcare domain. However, in the context of future research, our approach can be extended by observing related job profiles such as MTA and MA for validation purposes. Second, we limited our observational studies to German hospitals as a representative example of the healthcare domain. However, the assets we included in our analysis are rather broad (e.g., HIS, PDMS) and are assumed to be a part of any healthcare faculty. Third, since our approach is an extension of Schuetz et al.'s (2023) CSDM, our study is restricted by the same limitations.

6. Conclusion

This study used the first two steps of the ECD framework to develop a CSDM for IT-secure behavior in healthcare. For this purpose, several empirical analyses were conducted over three phases. Following this procedure, we extend the CSDM of Schuetz et al. (2023) with 33 healthcare-specific security threats, resulting in 1,120 threat vectors. Based on the reduced domain model, the CSDM for healthcare includes 114 relevant security threats. A risk assessment was then performed to determine the security threats that pose the most critical risks for employees working in the healthcare domain. This procedure resulted in 42 high or very high-risk threat vectors that can be used as a

blueprint for competence assessment and SETA program development beyond one-size-fits-all approaches in healthcare.

7. Acknowledgements

This research paper has been developed as part of the research project "KISK" funded by the German Federal Ministry of Health. We would like to thank the Federal Ministry of Health for its support.

8. References

Baker, L. (2006). Observation: A Complex Research Method. *Library Trends*, *55*(1), 171–189. https://doi.org/10.1353/lib.2006.0045

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Blank, R. M., & Gallagher, P. D. (2012). *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Blömeke, S., Gustafsson, J. E., & Shavelson, R. J. (2015). Beyond dichotomies: Competence viewed as a continuum. *Zeitschrift Fur Psychologie / Journal of Psychology*, *223*(1), 3–13. https://doi.org/10.1027/2151-2604/a000194

Bowling, A. (2014). *Research Methods in Health – Investigating Health and Health Services*. McGraw-hill education.

Bräutigam, C., Evans, M., Hilbert, J., & Öz, F. (2014). Arbeitsreport Krankenhaus eine Online-Befragung von Beschäftigten deutscher Krankenhäuser. *Hans-Böckler-Stiftung*, *No. 306*. http://hdl.handle.net/10419/116763

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud and Security*, *2016*(6), 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

Chiou, S.-T., Chiang, J.-H., Huang, N., & Chien, L.-Y. (2014). Health behaviors and participation in health promotion activities among hospital staff: Which occupational group performs better? *BMC Health Services Research*, *14*(1), 474. https://doi.org/10.1186/1472-6963-14-474

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59–71. https://doi.org/10.1007/s10551-008-9909-7

Denscombe, M. (2017). *EBOOK:The good research guide: For small-scale social research projects*. McGraw-Hill Education (UK).

Dincelli, E., & Chengalur-Smith, I. S. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, *29*(6), 669–687. https://doi.org/10.1080/0960085X.2020.1797546

Drevin, L., Kruger, H., Bell, A.-M., & Steyn, T. (2017). A linguistic approach to information security awareness education in a healthcare environment. *Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10*, 87–97. https://doi.org/10.1007/978-3-319-58553-6_8

ENISA. (2016). *Smart hospitals: Security and resilience for smart health service and infrastructures.* Publications Office. https://data.europa.eu/doi/10.2824/28801

Gerić, S., & Hutinski, Ž. (2007). Information System Security Threats Classifications. *Journal of Information and Organizational Sciences*, *30*(1), 51–61. https://hrcak.srce.hr/21445

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management*, *6*(1), 67–80. https://doi.org/10.36965/ojakm.2018.6(1)67-80

Göran, G. (2019). The Generation of Qualitative Data in Information Systems Research: The Diversity of Empirical Research Methods. *Communications of the Association for Information Systems*, 572–599. https://doi.org/10.17705/1CAIS.04428

Heikka, J. (2008). A constructive approach to information systems security training: An action research experience. *AMCIS 2008 Proceedings. 319*. https://aisel.aisnet.org/amcis2008/319

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

IBM Security. (2019). Cost of a Data Breach Report. *IBM Security*, 76.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). *Classification of security threats in information systems*. *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Klieme, E., Avenarius, H., Blum, W., Döbrich, P., Gruber, H., Prenzel, M., Reiss, K., Riquarts, K., Rost, J., Tenorth, H.-E., Vollmer, H. J., & Forschung, B. für B. und. (2003). *Zur Entwicklung nationaler Bildungsstandards. Eine Expertise*. Bonn, Berlin : BMBF. 10.25656/01:20901

Klotz, V. K., Winther, E., & Festner, D. (2015). Modeling the Development of Vocational Competence: A Psychometric Model for Economic Domains. *Vocations and Learning*, *8*(3), 247–268. https://doi.org/10.1007/s12186-015-9139-y

Kvist, T., Mäntynen, R., & Vehviläinen-Julkunen, K. (2013). Does Finnish hospital staff job satisfaction vary across occupational groups? *BMC Health Services Research*, *13*, 1–7. http://www.biomedcentral.com/1472-6963/13/376

Lehner, F. (2021). *Wissensmanagement*. Carl Hanser Verlag. https://doi.org/10.3139/9783446468115

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *Bmj*, *358*.

Maseti, O., & Pottas, D. (2006). A role-based security awareness model for South African hospitals.

Proceedings of the 6th Annual Information Security South Africa Conference, Sandton, South Africa, 5–7.
McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415
Mislevy, R. J. (2013). Evidence-Centered Design for Simulation-Based Assessment. *Military Medicine*, *178*(10 Suppl), 107–114. https://doi.org/10.7205/milmed-d-13-00213
Mislevy, R. J., & Haertel, G. D. (2006). Implications of Evidence-Centered Design for Educational Testing. *Educational Measurement: Issues and Practice*, *25*(4), 6–20. https://doi.org/10.1111/j.1745-3992.2006.00075.x
Motevali Haghighi, S., & Torabi, S. A. (2020). Business continuity-inspired fuzzy risk assessment framework for hospital information systems. *Enterprise Information Systems*, *14*(7), 1027–1060. https://doi.org/10.1080/17517575.2019.1686657
Rampold, F., Schütz, F., Masuch, K., Köpfer, P., & Warwas, J. (2022). Are you aware of your competencies? – The potentials of competence research to design effective SETA programs. *ECIS 2022 Research Papers. 134.*, 1–17. https://aisel.aisnet.org/ecis2022_rp/134
Sarantakos, S. (1998). *Social Research* (2nd Edition). MacMillan Education Australia.
Schuetz, F., Rampold, F., Köpfer, P., Mann, D., Trang, S., Masuch, K., & Warwas, J. (2023). Bridging the Gap between Security Competencies and Security Threats: Toward a Cyber Security Domain Model. *Proceedings. 56th Hawaii International Conference on System Sciences*, 10. https://hdl.handle.net/10125/103375
Schütz, F., Rampold, F., Kalisch, A., & Masuch, K. (2023). Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis. *Procedia Computer Science*, *219*, 521–528. https://doi.org/10.1016/j.procs.2023.01.320
Seeber, S. (2016). Vom Domänenmodell zum Kompetenzmodell: Konturen eines Assessmentdesigns zur Messung beruflicher Fachkompetenzen bei Medizinischen Fachangestellten. In *Bwp@ Berufs-und Wirtschaftspädagogik online* (pp. 1–25).
Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512
Statista. (2017). Umfrage zu Treibern der Veränderung in der IT-Sicherheit 2017. In *Statista*. https://de.statista.com/statistik/daten/studie/384321/umfrage/umfrage-zu-treibern-der-veraenderung-in-der-it-sicherheit/
Talib, Y. Y. A., & Dhillon, G. (2015). Employee ISP compliance intentions: An empirical test of empowerment. *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015*. https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/13/
Thomson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management and Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649
Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006
Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly: Management Information Systems*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01
Winther, E. (2010). *Kompetenzmessung in der beruflichen Bildung*. Bertelsmann.
Wunder, J., Halbardier, A., & Waltermire, D. (2011). *Specification for Asset Identification 1.1*. https://doi.org/10.6028/NIST.IR.7693

8. Appendix

	Work Task	Threat Event	Threat Area (Asset)
C1	Documentation of work with patients	Mishandling of critical and/or sensitive information	PDMS
C2		Salting the physical perimeter of organizations with removable media containing malware	USB Flashdrive
C3		Unauthorized internal information system access by insiders	PDMS
C4		Not locking the screen when being away from the PC	PC
C5	Organizational tasks	Deliver known malware to internal organizational information systems	Mail system
C6		Spear Phishing	Mail system
C7		Social engineering by outsiders to convince insiders to take harmful actions	Employee
C8	Work with patients	Spill sensitive Information (orally)	Employee
C9	Non-work-related tasks	Spill sensitive information	Instant messenger
C10		Spill sensitive information	Social Media Apps

Figure 6 Threat Vectors for Caregivers

	Work Task	Threat Event	Threat Area (Asset)
P1	Documentation of work with patients	Craft Counterfeit/spoof website	Internet Browser
P2		Mishandling of critical and/or sensitive information by authorized users	HIS
P3		Deliver known malware to internal organizational information systems	Internet Browser
P4		Unauthorized internal information system access by insiders.	HIS
P5	Organizational tasks	Mishandling of critical and/or sensitive information by authorized users	Smartphone
P6		Spear-Phishing	Mail system
P7		Use of unauthorized third-party hard and software	Employee
P8		Social engineering by insiders within organizations to convince other insiders to take harmful actions	Employee
P9	Non-work-related tasks	Spill sensitive information	Instant messenger
P10		Tailgate authorized staff to gain access to organizational facilities.	Physical Parameters

Figure 7 Threat Vectors for Physicians